Binary Quasi-differential Stochastic Process Keying Modulation Scheme for Covert Communications

Zhijiang XU [1,2], Suo ZHANG [1], Zhewei LIU [1], Jiliang LIN [1], Xiaoshuo HUANG [1], Yi GONG [2,3]

[1] School of Automation, Zhejiang Polytechnic University of Mechanical and Electrical Engineering, Binwen Rd. 528, 310053 Hangzhou, China
[2] Guangdong Provincial Key Laboratory of Advanced Wireless Communications, Xueyuan Rd. 1088, 518055 Shenzhen, China
[3] Department of Electrical and Electronic Engineering, Southern University of Science and Technology, Xueyuan Rd. 1088, 518055 Shenzhen, China

{xuzhijiang, zhangsuo, liuzhewei, linjiliang, huangxiaoshuo}@zime.edu.cn, gongy@sustech.edu.cn

Submitted August 27, 2024 / Accepted December 16, 2024 / Online first March 17, 2025

Abstract. *Covert communication working at the physical layer provides an important means for ensuring the security of private user data. This work proposes a novel covert communication system based on binary quasi-differential stochastic process keying (BQDSPK). At the transmitter, the polarity of the correlation coefficient of two consecutive stochastic sequences is modulated by one binary covert bit. At the receiver, the correlation between two consecutively received random sequences is computed, and the transmitted covert bit is inferred through a hard decision process. A pseudo-random sequence is introduced to eliminate the transmitted sequences' correlation. The transmitted signal has the same statistical characteristics as the ambient noise to avoid attracting the attention of eavesdroppers. We theoretically demonstrate that the proposed system fully satisfies the requirement of covert communication when the signal-to-noise ratio (SNR) is less than a certain threshold value. In addition, theoretical bit error rate (BER) expressions are derived under additive white Gaussian noise (AWGN) channels and frequency-flat fading channels. The simulation results show that the theoretical BERs are very close to the BERs obtained from the simulations, regardless of which stochastic process is used as the carrier. Specifically, when the number of samples within a bit period is* 400*, the BER approaches approximately* 10^{-5} *at a SNR of* -5 *dB under an AWGN channel, which adequately satisfies the communication requirements.*

Keywords

Physical layer covert communication, stochastic process, pseudo-random sequence, modulation, correlation

1. Introduction

Due to the broadcast and open nature of wireless channels, information security is an even more critical issue that cannot be ignored [1–3]. Previously, the information security protection either relied on the steganography [4] at the application layer or the physical layer security (PLS) [5] at the physical layer. However, given the constraints of resources available for low-cost Internet of Things (IoT) end devices, conventional steganography and PLS are insufficient to address all security challenges within IoT systems [6], and users' privacy concerns still need to be fully alleviated. Covert communication, milestone research conducted by Bash et al. [7], can provide a higher level of security to transmitters, which hides the very existence of transmission from the detection of adversaries [8], [9]. An eavesdropper will disregard these "signals" as mere background noise and will not utilise resources to tackle them. Applying the concept of covert communication to wireless transmission enables the concealment of user information within "noise", including environmental or artificial interference, thus mitigating privacy risks.

1.1 Related Works

Physical layer-based wireless covert channels can be categorized into two types: coding-based wireless covert channels and modulation-based wireless covert channels [10]. This work focuses on the latter.

Research on intelligent reflecting surface (IRS)-assisted covert communication has been carried out recently [11–14]. Specifically, the authors in [11] investigated the multi-input multi-output (MIMO) covert communication aided by IRS against a multi-antenna warden. In [12], the authors inspired by the great success of deep reinforcement learning (DRL) in handling challenging optimization problems, DRL adjusted the transmit beamformer vector and phase shifts matrixis of IRS to maximum covert communication performance. In [13], the authors proposed a novel aerial reconfigurable intelligent surface-assisted covert communication framework to enhance the covert performance of ground transceivers in the presence of a warden. Combined with other techniques, such as non-orthogonal multiple access (NOMA) [14], covert

DOI: 10.13164/re.2025.0064

communications can further help to improve wireless security while guaranteeing transmission performance. These solutions may not be suitable for low-cost IoT devices lacking MIMO RF modules and insufficient supercomputing power to implement DRL.

In practical IoT systems, relays are often necessary, where one device can send information to another device through multiple relays. Works [15–17] show that relay-assisted schemes can significantly improve covert performance both in terms of detection error probability and covert capacity. Two relay selection schemes are considered in [15], [16], and theoretical analysis shows that the covert capacity under the superior-link selection scheme is always higher than that under the random selection scheme. In [17], an energy-efficient covert communication scheme with an adaptive assist nodes group based on a uniform jamming power strategy against the joint-phase detection of the eavesdropper is proposed.

Many existing works exploited the noise uncertainty for covert communication, the work [18] demonstrates that the covert performance gain stemming from the noise uncertainty is indeed fragile when the eavesdropper has multiple antennas. The work [19] adopts the channel reverse power control technology to ensure the constant signal power of the receiver, and the noise uncertainty at the eavesdropper serves as the enabler of covert communications. Work [20] proposes a strategy that allows legitimate users to communicate reliably and secretly, where the friendly node closest to the adversary, not being closely coordinated with Alice, generates artificial noise. Work [21] explicitly reveals that a higher covert rate can be achieved when the adversary does not know the transmitter's location.

A stochastic process rather than a conventional sine wave is used as a carrier and one of the characteristic parameters of the carrier is modulated by a covert bit for covert communication in works [22–28]. Due to the non-periodic nature of the random process and its statistical characteristics resembling environmental noise, it is challenging to capture the adversary's attention for covert communication purposes. In works [22–25], the covert bits modulate the characteristic exponent α or skewness β of the alpha-stable distribution. However, the main problem is that the estimation complexity of the parameters α, β is very high, while the estimation accuracy is not high. Xu et al. in [26] proposed a covert communication scheme where the correlation coefficients of two consecutive Gaussian sequences were modulated by a covert bit. Another scheme was proposed in [27] that a non-zero mean Gaussian sequence was used as a carrier, and the mean value of the carrier was modulated by a covert bit. In this work, we extend the carrier from a Gaussian-distributed stochastic process to stochastic processes with fourth-order moments, and a pseudo-random sequence is added to further reduce the autocorrelation of the covert signal. Basar in [28] proposed the concept of noise modulation (NoiseMod) and gave an example of transmitting covert bits with Gaussian noise of different variances. However, this scheme is easily detected because fluctuations in the noise variance are easily distinguishable from the time domain.

1.2 Contributions

This work proposes a novel covert communication scheme based on binary quasi-differential stochastic process keying. Any stochastic process with a fourth-order central moment, rather than a traditional sine wave, is used as a carrier. At the transmitter, the polarity of the correlation coefficient of two consecutive stochastic sequences is modulated by one binary covert bit. Here, the selected correlation coefficient is close to but not equal to 1, which is called a binary quasi-differential stochastic process keying (BQDSPK) modulation. The purpose of this design is that, on the one hand, the correlation coefficient is not equal to 1, making the random carriers in the two adjacent bit periods different to increase the confusion of the eavesdropper. On the other hand, the correlation coefficient should be as close to 1 as possible to reduce the bit error rate of legitimate users. Furthermore, a pseudo-random sequence is introduced to prevent the eavesdropper from using correlation to detect the presence of covert signals. At the receiver, a correlation is made between the two received consecutive stochastic sequences, and the covert bit is estimated by hard decision. Our main contributions can be summarized as follows:

- A novel covert communication scheme based on BQDSPK is proposed. Any stochastic process with a fourth-order central moment can be used as a carrier. More importantly, the transmitted signal obeys a normal distribution after several bit periods, irrespective of the specific stochastic process chosen as the carrier. The transmitted signal has the same statistical characteristics as the ambient noise to avoid attracting the attention of eavesdroppers. Further, the proposed covert communication system has a simple structure and low computational complexity, which is well suited for low-cost IoT devices.

- Based on the theoretical analysis of the proposed covert communication system, it is observed that when the SNR falls below a certain threshold, complete covertness is achieved, i.e., the eavesdropper is unable to determine whether the legitimate user is sending data or not.

- The theoretical BER of the system is derived under additive white Gaussian noise (AWGN) and quasi-static fading channels, respectively. Extensive simulations are conducted to evaluate our proposed covert system's performance. Simulation results are very consistent with the theoretical derivation.

1.3 Organization

The rest of this work is organized as follows. The proposed covert communication scheme is presented in Sec. 2. In Sec. 3, the probability density function (PDF) of correlator outputs under AWGN and quasi-static fading channels is derived, respectively. We examine the performance of covertness and BER in Sec. 4. Using correlation detection, we study the synchronization of receivers in Sec. 5. Extensive numerical calculations and Monte Carlo simulations are presented to evaluate the performance of the proposed scheme in Sec. 6, and we present conclusions in Sec. 7.

2. Covert Communication Scheme

In this section, we briefly introduce the definition of the Pearson correlation coefficient for two stochastic processes and then present the proposed communication system.

2.1 Pearson Correlation Coefficient

Two mutually independent stochastic processes $\theta(t)$ and $\epsilon(t)$ with second-order moments, the Pearson correlation coefficient ρ is defined as

$$\begin{aligned}\rho &= \frac{\mathbb{E}\left[(\theta(t)-\mu_\theta)\,(\epsilon(t)-\mu_\epsilon)\right]}{\sigma_\theta\sigma_\epsilon} \\ &= \mathbb{E}\left[\frac{\theta(t)-\mu_\theta}{\sigma_\theta}\,\frac{\epsilon(t)-\mu_\epsilon}{\sigma_\epsilon}\right] \triangleq \mathbb{E}\left[\theta^*(t)\epsilon^*(t)\right]\end{aligned} \tag{1}$$

where μ_θ (μ_ϵ) and σ_θ (σ_ϵ) are the mean and standard deviation of the stochastic process $\theta(t)$ ($\epsilon(t)$), respectively. Thus, given two mutually independent and standardized stochastic processes $\theta^*(t)$ and $\epsilon^*(t)$, a stochastic process $\lambda^*(t)$ can be constructed such that $\theta^*(t)$ and $\lambda^*(t)$ have a correlation coefficient $\rho \in [-1, 1]$. The expression $\lambda^*(t)$ can be written as

$$\lambda^*(t) = \rho\theta^*(t) + \sqrt{1-\rho^2}\epsilon^*(t). \tag{2}$$

In particular, when both $\theta(t)$ and $\epsilon(t)$ obey the same distribution and their means are zero, then there is no need to standardize $\theta(t)$ and $\epsilon(t)$. The stochastic process $\lambda^*(t)$ is rewritten as $\lambda(t)$ and Equation (2) simplifies to

$$\lambda(t) = \rho\theta(t) + \sqrt{1-\rho^2}\epsilon(t). \tag{3}$$

2.2 BQDSPK Modulation

In the proposed covert communication scheme shown in Fig. 1, a covert bit is encoded by the correlation coefficients ρ of two adjacent stochastic sequences. Then the corresponding stochastic sequences are transmitted through the channel. The purpose of the introduced pseudo-random sequences is to eliminate the correlation of the transmitted sequences $\lambda(t)$, which is elaborated in Sec. 5 and need not be considered here. More specifically, independent identically distributed random sequences $\epsilon(t)$ are generated by the stochastic process generator within a covert bit period T_b, independent of the delayed predecessor distribution sequences $\theta(t)$. During the bit period T_b, a stochastic sequences, $\lambda(t) = (-1)^b\rho\theta(t) + \sqrt{1-\rho^2}\epsilon(t)$, are transmitted, where the covert bit $b \in \{0, 1\}$. For the sake of description, we assume that the covert bit $b = 0$ is sent, such that $(-1)^b\rho$ is written directly as ρ.

It can be seen from the structure of the modulator that the transmitted signals are statistically identical regardless of whether they are consecutively the same or different covert bits. The modulated signals generated by the transmitter in this way, have completely different waveforms in the time domain, but the spectrum is the same. This makes it impossible for illegal eavesdroppers to determine whether a signal exists easily, and even more difficult to demodulate the '0' or/and '1' bit streams.

2.3 BQDSPK Demodulation

Since the signals received by the receiver within two adjacent bit periods are correlated, the received signals are delayed by a one-bit period as shown in Fig. 1. The signal of the previous bit period is correlated with the signal of the following bit period and then compared with the threshold 0 for hard decision. A value greater than 0 is decided as bit '0', and a value less than 0 is chosen as bit '1', thus greatly simplifying the demodulation process. The pseudo-random sequence synchronization module is a critical component within the receiver. If the pseudo-random sequences of both the transmitter and receiver are not synchronized, there will be no correlation between the received sequences across two consecutive bit peroid, thereby preventing accurate demodulation. In Sec. 5.3, we present a detailed solution to the synchronization challenge associated with pseudo-random sequences.

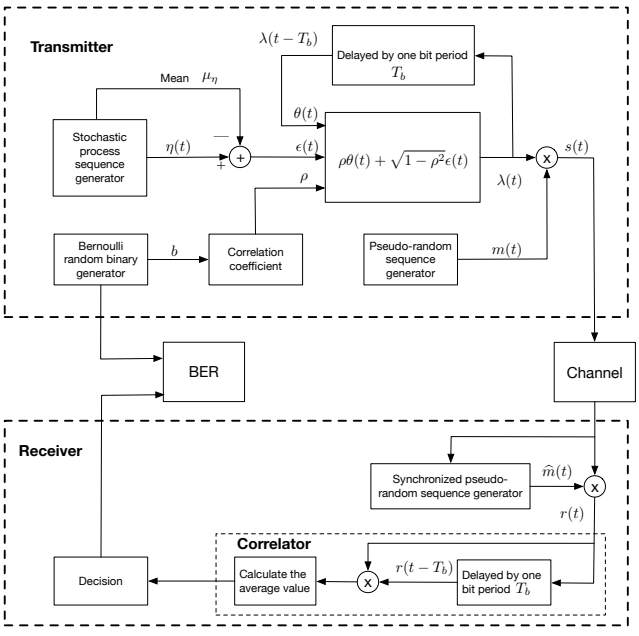


Fig. 1. The block diagram of the proposed covert communication system.

2.4 Complexity Analysis

Assuming that there are ν samples in a bit period T_b. The BQDSPK modulator depicted in Fig. 1, in addition to the stochastic process generator for the carrier and the Bernoulli binary random bit generator for producing covert bits, incorporates a remaining modulation signal module as represented by (3) and a delayed one-bit period module, both of which exhibit very low computational complexity as they are only multiplication and addition operations. Specifically, Equation (3) requires 2ν floating-point multiplications and ν floating-point additions. In the demodulator, the computational complexity of the correlator is also very low, involving only ν floating-point multiplications and ν floating-point additions. At the demodulator, it is the pseudo-random sequence synchronisation module that has the greater computational complexity. Let us denote the length of the pseudo-random sequence as m. In Sec. 5.3, it is stated that at most m correlation operations, specifically $m\nu$ floating-point multiplications and $m\nu$ floating-point additions, are required to achieve synchronization of a pseudo-random sequence with the transmitter. Nevertheless, synchronization of the pseudo-random sequences occurs infrequently. Consequently, the computational complexity associated with the synchronization module remains relatively low.

3. PDF of Correlator Output

We first derive the PDF of the modulating signal for the k-th covert bit, and then give the PDF of the correlator output under AWGN channels and quasi-static fading channels, respectively.

3.1 Distribution of modulated signal

Referring to the transmitter modulation process shown in Fig. 1, the sequence of the k-th covert bit within the bit period T_b is denoted as $\lambda(t + kT_\mathrm{b})$. For ease of writing, $\lambda(t + kT_\mathrm{b})$ is abbreviated as λ_k and $\epsilon(t + kT_\mathrm{b})$ is abbreviated as ϵ_k. According to the modulation process of the proposed transmitter, we have

$$\begin{cases} \lambda_0 = \epsilon_0 \\ \lambda_1 = (-1)^{b_1}\rho\epsilon_0 + \sqrt{1-\rho^2}\epsilon_1 \\ \qquad \vdots \\ \lambda_k = (-1)^{b_k}\rho\lambda_{k-1} + \sqrt{1-\rho^2}\epsilon_k \\ \qquad \vdots \end{cases} \tag{4}$$

where $\epsilon_i = \eta_i - \mu_\eta$, and $b_i \in \{0, 1\}$ is the i-th covert bit. Here $\lambda_0 = \epsilon_0$ serves as the reference carrier and contains no covert bit. The stochastic process $\eta(t)$ has a central moment of order 1 to 4, denoted as $\{c_i, i = 1, \cdots, 4\}$. The central moments are defined as

$$c_i = \int_{-\infty}^{+\infty} (x - \mu_\eta)^i f(x)\mathrm{d}x \tag{5}$$

where $f(x)$ is the PDF, and $\mu_\eta = \int_{-\infty}^{+\infty} x f(x)\mathrm{d}x$ is the mean of the stochastic process $\eta(t)$. Clearly, the variance of $\epsilon(t)$ is the variance of $\eta(t)$, i.e., $\sigma_\epsilon^2 = \sigma_\eta^2$. Further, with the definition of the central moment, it follows that $c_1 = 0$.

From the expression in (4), it can be seen that the expression for the PDF of the modulated signal λ_k is very complex, except for the fact that the stochastic process ϵ_i is normally distributed. To better obtain the distribution of the stochastic process λ_k, we rewrite (4) as follows

$$\begin{aligned} \lambda_k &= (-1)^{b_k}\rho\lambda_{k-1} + \sqrt{1-\rho^2}\epsilon_k \\ &= (-1)^{b_k}\rho\left((-1)^{b_{k-1}}\rho\lambda_{k-2} + \sqrt{1-\rho^2}\epsilon_{k-1}\right) + \sqrt{1-\rho^2}\epsilon_k \\ &\quad \vdots \\ &= (-1)^{\sum_{j=1}^{k} b_j}\rho^k\epsilon_0 + \sqrt{1-\rho^2}\sum_{i=1}^{k}(-1)^{\sum_{j=i+1}^{k} b_j}\rho^{k-i}\epsilon_i \\ &= (-1)^{m_0}\rho^k\epsilon_0 + \sqrt{1-\rho^2}\sum_{i=1}^{k}(-1)^{m_i}\rho^{k-i}\epsilon_i \end{aligned} \tag{6}$$

where $m_i \triangleq \sum_{j=i+1}^{k} b_j \bmod 2$ and $m_k \triangleq 0$. It should be a $(k+1)$-fold convolution of $\epsilon(t)$ since $\{\epsilon_i, i = 0, \cdots, k\}$ are mutually independent and identically distributed stochastic processes. Fortunately, when k is sufficiently large (e.g., $k > 5$), then by the Central Limit Theorem (CLT), the PDF of λ_k tends to be normally distributed, i.e., $\lambda_k \sim \mathcal{N}(0, \sigma_\lambda^2)$. Its mean is 0 and its variance is

$$\begin{aligned} \sigma_\lambda^2 &= \mathbb{E}[\lambda_k^2] \\ &= \rho^{2k}\mathbb{E}[\epsilon_0^2] + \left(1-\rho^2\right)\sum_{i=1}^{k}\rho^{2(k-i)}\mathbb{E}\left[\epsilon_i^2\right] \\ &= \sigma_\epsilon^2\left[\rho^{2k} + \left(1-\rho^2\right)\sum_{i=0}^{k-1}\rho^{2i}\right] = \sigma_\epsilon^2 = \sigma_\eta^2 = c_2. \end{aligned} \tag{7}$$

Therefore, the PDF of the modulated signal λ_k is approximated as

$$f_\lambda(x) = \frac{1}{\sqrt{2\pi}\sigma_\eta}\mathrm{e}^{-\frac{x^2}{2\sigma_\eta^2}}, \tag{8}$$

regardless of which distribution the stochastic process $\eta(t)$ obeys. Thus, the fourth-order moment of λ_i is $\mathbb{E}[\lambda_i^4] = 3\sigma_\eta^4$.

3.2 Distribution of Correlator Outputs under AWGN Channels

Assuming two stochastic processes with a correlation coefficient of ρ under a white Gaussian noise channel, the expression is written as

$$\begin{cases} r_{k-1} = \lambda_{k-1} + n_{k-1} \\ r_k = \rho\lambda_{k-1} + \sqrt{1-\rho^2}\epsilon_k + n_k \end{cases} \tag{9}$$

where $r_i = r(t + iT_\mathrm{b}), n_i = n(t + iT_\mathrm{b})$ are the received signal and noise in the i-th bit period, respectively. The channel

noise follows a normal distribution with mean 0 and variance σ_n^2, i.e., $n_i \sim \mathcal{N}(0, \sigma_n^2)$, and n_i, λ_i are mutually independent stochastic processes.

Let $\zeta_k = r_{k-1} r_k$, and there is

$$\begin{aligned}\zeta_k = {} & \rho\lambda_{k-1}^2 + \sqrt{1-\rho^2}\lambda_{k-1}\epsilon_k + \rho\lambda_{k-1}n_{k-1} \\ & + \sqrt{1-\rho^2}\epsilon_k n_{k-1} + \lambda_{k-1}n_k + n_{k-1}n_k.\end{aligned} \tag{10}$$

Using the mutual independence of $\lambda_{k-1}, \epsilon_k, n_{k-1}, n_k$ and $\mathbb{E}[n_i] = \mathbb{E}[\lambda_i] = \mathbb{E}[\epsilon_i] = 0$, we obtain the first-order and 2nd-order origin moments of ζ, respectively, are

$$\mu_\zeta = \mathbb{E}[\zeta_k] = \rho c_2 = \rho\sigma_\eta^2 \tag{11}$$

and

$$\begin{aligned}\mathbb{E}[\zeta_k^2] &= \rho^2\mathbb{E}[\lambda_{k-1}^4] + (1-\rho^2)c_2^2 + \sigma_n^4 + 2\sigma_n^2 c_2 \\ &= 3\sigma_\eta^4\rho^2 + (1-\rho^2)\sigma_\eta^4 + \sigma_n^4 + 2\sigma_n^2\sigma_\eta^2.\end{aligned} \tag{12}$$

This gives the variance of ζ_k as

$$\sigma_\zeta^2 = \underbrace{(1+\rho^2)\sigma_\eta^4}_{\sigma_{\zeta_\mathrm{s}}^2} + \underbrace{\left(2\sigma_\eta^2 + \sigma_n^2\right)\sigma_n^2}_{\sigma_{\zeta_\mathrm{i}}^2}. \tag{13}$$

Let the number of samples in a covert bit period T_b be ν. Assuming that the receiver has been synchronized, and combined with (10), this yields the k-th output of the receiver correlator $z_k = \frac{1}{\nu}\sum_{j=1}^{\nu}\zeta_{k,j} = z_{k,\mathrm{s}} + z_{k,\mathrm{i}}$, i.e.,

$$\begin{aligned}z_{k,\mathrm{s}} &= \frac{1}{\nu}\sum_{j=1}^{\nu}\left(\rho\lambda_{k-1,j}^2 + \sqrt{1-\rho^2}\lambda_{k-1,j}\epsilon_{k,j}\right) \\ z_{k,\mathrm{i}} &= \frac{1}{\nu}\sum_{j=1}^{\nu}\Big(\rho\lambda_{k-1,j}n_{k-1,j} + \sqrt{1-\rho^2}\epsilon_{k,j}n_{k-1,j} \\ &\qquad + \lambda_{k-1,j}n_{k,j} + n_{k-1,j}n_{k,j}\Big)\end{aligned} \tag{14}$$

where $\lambda_{k,j}$ is the j-th sample of the stochastic process λ_k, and $n_{k,j}$ is the j-th sample of the channel noise n_i. Equation (14) indicates that the k-th output z_k of the correlator is known as the sum of the signal component $z_{k,\mathrm{s}}$ and the interference component $z_{k,\mathrm{i}}$. The distribution of the signal component $z_{k,\mathrm{s}}$ is determined by the stochastic process employed by the carrier. However, when the number of samples ν is sufficiently large, and assuming that the stochastic process chosen by the carrier has fourth-order moments, z_k converges to a normal distribution according to the central limit theorem. Combining (11) and (13), the mean and variance of z_k are

$$\begin{cases}\mu_z = \mu_\zeta = \rho\sigma_\eta^2 \\ \sigma_z^2 = \dfrac{1}{\nu}\sigma_\zeta^2 = \underbrace{\nu^{-1}\sigma_{\zeta_\mathrm{s}}^2}_{\sigma_{z_\mathrm{s}}^2} + \underbrace{\nu^{-1}\sigma_{\zeta_\mathrm{i}}^2}_{\sigma_{z_\mathrm{i}}^2}\end{cases} \tag{15}$$

respectively.

The following is an example of a stochastic process with a Gaussian distribution for the carriers to show that the signal component z_s converges to a normal distribution. Given that the carrier $\eta(t)$ obeys the $\mathcal{N}(0, \sigma_\eta^2)$ distribution with a correlation coefficient of 1 ($\rho = 1$), z_s obeys the central chi-square distribution, i.e.,

$$f_{z_\mathrm{s}}(x) = \frac{\nu}{\sigma_\eta^2}\left(\frac{x\nu}{\sigma_\eta^2}\right)^{(\nu-2)/2} \mathrm{e}^{-\frac{x\nu}{2\sigma_\eta^2}} \frac{1}{2^{\nu/2}\Gamma(\nu/2)}. \tag{16}$$

When ν is large, then the central chi-square distribution converges to a normal distribution with mean and variance obtained by the CLT, which gives

$$\mu_{z_\mathrm{s}} = \sigma_\eta^2,\ \sigma_{z_\mathrm{s}}^2 = 2\sigma_\eta^4\nu^{-1}. \tag{17}$$

That is, the PDF of the signal component z_s at the output of the correlator is approximated as

$$f_{z_\mathrm{s}}(x) \cong \frac{1}{\sqrt{4\pi\sigma_\eta^4\nu^{-1}}}\mathrm{e}^{-\frac{\left(x-\sigma_\eta^2\right)^2}{4\sigma_\eta^4\nu^{-1}}}. \tag{18}$$

From the PDF of z_s, Equation (18), it can be seen that when the number of samples ν increases, the mean remains constant but the variance decreases. Taking the number of samples $\nu = 100$, the second-order power $\sigma_\eta^2 = 1$, and the correlation coefficient $\rho = 1$ as an example, the PDF of the chi-square distribution and the normal distribution are given in Fig. 2, from which it can be seen that they are very close to each other. Indeed, according to the CLT, the chi-square distribution must be approximated to a normal distribution when ν is large enough.

In communications theory, Nakagami distributions, Rice/Rician distributions, and Rayleigh distributions are commonly used to model scattered signals that arrive at a receiver via multiple paths. Depending on the density of the scatter, the signal will show different attenuation characteristics. The Rayleigh and Nakagami distributions are used to model dense scatters, while the Rician distributions are used to model fading with a stronger line-of-sight. The Nakagami distributions can be reduced to the Rayleigh distributions, but have more control over the degree of the fading. Table 1 lists the common stochastic processes, and the corresponding PDFs and parameters, subject to the unit variance constraint.

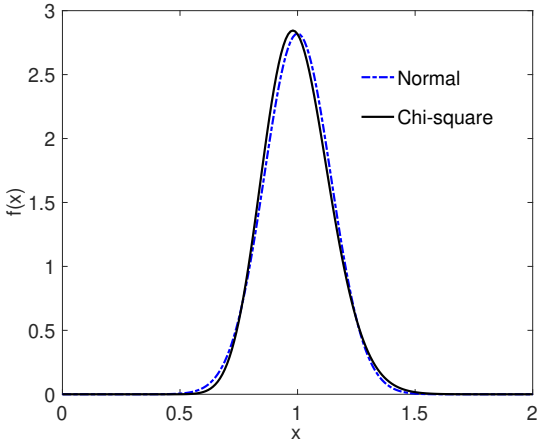


Fig. 2. PDF and convergence function of z_s when the carrier uses a normally distributed stochastic process.

Distribution	PDF
Uniform	$f(x) = 1/\sqrt{12}, \lvert x\rvert \le \sqrt{3}$
Normal	$f(x) = \frac{1}{\sqrt{2\pi}}\mathrm{e}^{-(x-\mu)^2/2}, x \in \Re$
Laplace	$f(x) = \frac{1}{\sqrt{2}}\mathrm{e}^{-\sqrt{2}\lvert x-\mu\rvert}, x \in \Re$
Exponential	$f(x) = \mathrm{e}^{-x}, x \ge 0$
Rayleigh	$f(x) = (2-\frac{\pi}{2})x\mathrm{e}^{-(1-\frac{\pi}{4})x^2}, x \ge 0$
Gamma	$f(x) = \frac{\alpha^{\alpha/2}x^{\alpha-1}}{\Gamma(\alpha)}\mathrm{e}^{-\sqrt{\alpha}x}$, $x \ge 0, \alpha > 0$
LogNormal	$f(x) = \frac{1}{\sqrt{2\pi}\sigma x}\mathrm{e}^{-\frac{(\log(x)-\mu)^2}{2\sigma^2}}, x > 0$, $\mu = -\frac{1}{2}\log(2), \sigma = \sqrt{\log(2)}$
Weibull	$f(x) = \frac{\alpha}{\beta}\left(\frac{x}{\beta}\right)^{\alpha-1}\mathrm{e}^{-\left(\frac{x}{\beta}\right)^{\alpha}}$, $x \ge 0, \alpha > 0$, $\beta = \left(\Gamma\left(1+\frac{2}{\alpha}\right) - \Gamma\left(1+\frac{1}{\alpha}\right)^2\right)^{-1/2}$
Rician/Rice*	$f(x) = I_0\left(\frac{x\alpha}{\beta^2}\right)\frac{x}{\beta^2}\mathrm{e}^{-\left(\frac{x^2+\alpha^2}{2\beta^2}\right)}, x \ge 0$ $\alpha \ge 0, \beta > 0$
Chi-square*	$f(x) = \frac{2^{-\nu/2}}{\Gamma(\nu/2)}\mathrm{e}^{-x/2}x^{\nu/2-1}$, $x \ge 0, \nu \ge 3$
Nakagami*	$f(x) = \frac{2}{\Gamma(\mu)}\left(\frac{\mu}{\omega}\right)^{\mu}x^{2\mu-1}\mathrm{e}^{-x^2\mu/\omega}$, $x \ge 0, \mu > 0, \omega > 0$

* The generated random sequence needs Z-Score normalization (observation minus mean divided by standard deviation). The chi-square distribution has a mean of ν and a variance of 2ν. The Nakagami distribution has a mean of $\sqrt{\omega/\mu}\Gamma\left(\frac{1}{2}+\mu\right)/\Gamma(\mu)$ and a variance of $\omega\left(1-\frac{\Gamma\left(\frac{1}{2}+\mu\right)^2}{\mu\Gamma(\mu)^2}\right)$. The expressions for the mean and variance of the Rician distribution are more complicated and will not be written out here.

Tab. 1. PDFs of some common stochastic processes used as carriers, which are all set to unit variance.

3.3 Distribution of Correlator Outputs under Quasi-static Fading Channels

In wireless communication, the channel is always fading. To further evaluate the performance of the proposed binary differential stochastic process keying system, the channel is assumed to be slow fading in this work. The so-called "slow fading" is relative to the covert bit period T_b, and it is assumed that the channel gain remains unchanged during the two consecutive covert bit periods, which is considered to be a non-zero real constant. The observed signals in the two consecutive T_b are

$$\begin{cases} r_{k-1} = h\lambda_{k-1} + n_{k-1} \\ r_k = h\left(\rho\lambda_{k-1} + \sqrt{1-\rho^2}\epsilon_k\right) + n_k \end{cases} \tag{19}$$

where the fading coefficient h is a real random variable obeying a certain distribution and is independent of the carrier and the noise.

Similar to the derivation of the probability density function of the correlator output under additive white Gaussian channels in Sec. 3.2, we obtain that the correlator output under quasi-static fading channels obeys a normal distribution distribution. Its mean and variance are

$$\mu_z = h^2\rho\sigma_\eta^2 \tag{20}$$

and

$$\sigma_z^2 = \nu^{-1}h^4\left(1+\rho^2\right)\sigma_\eta^4 + \nu^{-1}\left(2h^2\sigma_\eta^2 + \sigma_n^2\right)\sigma_n^2, \tag{21}$$

respectively. Therefore, its PDF can be written as

$$f_z(z|h) = \frac{1}{\sqrt{2\pi}\sigma_z}\mathrm{e}^{-\frac{\left(z-h^2\rho\sigma_\eta^2\right)^2}{2\sigma_z^2}}. \tag{22}$$

4. Theoretical Derivation of System Performance

Without loss of generality, it is assumed that a Z-Score normalization is performed on the transmitted carrier, i.e., the variance of the stochastic carrier $\sigma_\eta^2 = 1$. It should be emphasized that the variance, rather than the second-order moments of origin, is chosen as the carrier power here, taking into account the fact that some stochastic processes do not have a mean of 0, such as the exponential distribution.

Since the carrier is a stochastic process, the SNR ξ is defined as the ratio of the variance of the carrier to the variance of the noise, i.e.,

$$\xi = \frac{\sigma_\eta^2}{\sigma_n^2} \tag{23}$$

where σ_η^2 and σ_n^2 are the variance of the carrier and the noise, respectively.

4.1 Covertness

To determine whether the legitimate user is transmitting, the eavesdropper faces a binary hypothesis test (i.e., the null hypothesis $\mathcal{H}_0$ and the alternative hypothesis $\mathcal{H}_1$), where $\mathcal{H}_0$ indicates that the legitimate user is silent and $\mathcal{H}_1$ indicates that the legitimate user is transmitting covert information. Disregarding the issues of synchronization and signal fading, since the modulated signal obeys a normal distribution and is independent of the noise, the signal received by the eavesdropper is

$$r_\mathrm{e}(t) = \begin{cases} n(t) \sim \mathcal{N}(0, \sigma_n^2), & \mathcal{H}_0 \\ \lambda(t) + n(t) \sim \mathcal{N}(0, \sigma_\eta^2 + \sigma_n^2), & \mathcal{H}_1 \end{cases}. \tag{24}$$

During the listening period, the eavesdropper segments the observed samples into non-overlapping sub-sequences of length ν, then the average signal power is given by

$$\Lambda = \frac{1}{\nu}\sum_{i=1}^{\nu} r_{\mathrm{e},i}^2 \tag{25}$$

where $r_{\mathrm{e},i}$ is the i-th sample of $r_\mathrm{e}(t)$. Based on the average signal power, the eavesdropper's binary hypothesis detection can be rewritten as

$$\Lambda \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \Lambda_0 \tag{26}$$

where Λ_0 denotes eavesdropper's testing threshold. Since $\{r_{e,i}\}$ are independent of each other, the average signal power Λ obeys a central chi-square distribution with ν of freedom. By utilizing (16)–(18), Λ can be approximated to follow a normal distribution and has

$$\Lambda \sim \begin{cases} \mathcal{N}(\sigma_n^2, 2\nu^{-1}\sigma_n^4), & \mathcal{H}_0 \\ \mathcal{N}\left((1+\xi)\sigma_n^2, 2\nu^{-1}(1+\xi)^2\sigma_n^4\right), & \mathcal{H}_1 \end{cases}. \tag{27}$$

The detection error probabilities are widely used to measure the eavesdropper's performance. When a transmitter covertly sends a message to a legitimate user, and the eavesdropper incorrectly determines that there is no communication based on the strength of the received signal, we have a missing detection with the possibility of $\mathbb{P}_{\mathrm{MD}}$. Furthermore, when the sender does not transmit covert information to the legitimate receiver, but the eavesdropper erroneously concludes that communication is taking place, we have a false alarm with the possibility of $\mathbb{P}_{\mathrm{FA}}$. As a result, the eavesdropper's detection error probability is given by

$$\mathbb{P}_{\mathrm{e}}^{(w)} = p_0\mathbb{P}_{\mathrm{MD}} + p_1\mathbb{P}_{\mathrm{FA}} \tag{28}$$

where p_i is the prior probability of $\mathcal{H}_i$. Substituting (27) into (28) and making $\frac{\mathrm{d}\mathbb{P}_{\mathrm{e}}^{(w)}}{\mathrm{d}\Lambda_0} = 0$ to yield the optimal threshold Λ_0^* that minimizes the probability of detection error by the eavesdropper, and then substituting Λ_0^* into (28) yields the minimum probability of detection error for the eavesdropper. After simplification and approximation, the minimum $\mathbb{P}_{\mathrm{e}}^{(w)}$ is obtained as

$$\begin{aligned} \mathbb{P}_{\mathrm{e,min}}^{(w)} \approx \frac{p_0}{2}\left(1+\mathrm{Erf}\left(-\sqrt{\frac{(\xi+1)^2}{\xi(\xi+2)}\log\left(\frac{(\xi+1)p_0}{p_1}\right)}\right)\right) \\ + \frac{p_1}{2}\mathrm{Erfc}\left(-\sqrt{\frac{1}{\xi(\xi+2)}\log\left(\frac{(\xi+1)p_0}{p_1}\right)}\right) \end{aligned} \tag{29}$$

where the complementary error function of x is defined as $\mathrm{Erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty \mathrm{e}^{-t^2}\mathrm{d}t$, and the error function $\mathrm{Erf}(x) = 1 - \mathrm{Erfc}(x)$. We note that covert communication constraint requires $\mathbb{P}_{\mathrm{e}}^{(w)} \geq \min(p_0, p_1) - \varepsilon$, where ε is an arbitrarily small positive value [7]. We assume that the probability of covert transmission is much less than that of no transmission, i.e., $p_1 \ll p_0$. Let's take $p_1 = 1/8$ as an example, and the curve of the relationship between SNR ξ and detection error probability $\mathbb{P}_{\mathrm{e,min}}^{(w)}$ is plotted according to (29), as shown in Fig. 3. As can be seen from the figure, when the SNR ξ is less than -7 dB, then the detection error probability $\mathbb{P}_{\mathrm{e,min}}^{(w)} \approx 1/8 = \min(p_0, p_1)$, which fully meets the requirement of covert communication.

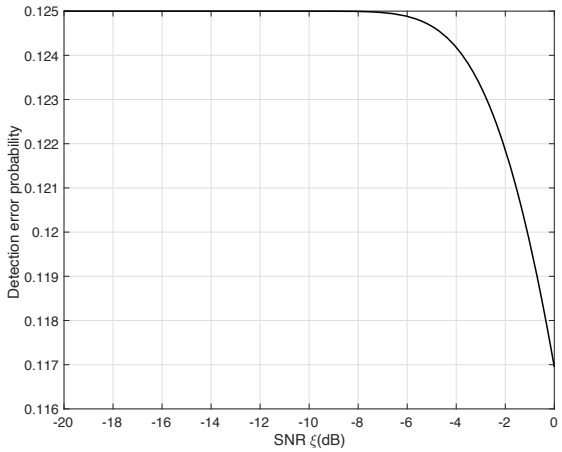


Fig. 3. Minimum probability of detection error for the eavesdropper, where $p_0 = \frac{7}{8}$ and $p_1 = \frac{1}{8}$.

Kullback-Leibler divergence (K-L) [29] is used to measure statistics that quantify the proximity of two probability distributions in the same event space. The Kullback-Leibler divergence of Q from P is defined to be

$$D_{\mathrm{KL}}(P||Q) = \int_{-\infty}^{\infty} p(x)\log\left(\frac{p(x)}{q(x)}\right)\mathrm{d}x \tag{30}$$

where $p(x)$ and $q(x)$ denote the PDFs of the random variables P and Q, respectively. When P and Q have the same probability distribution, the K-L distance is 0. Here, let $p(x)$ be the PDF under the $\mathcal{H}_0$ assumption and $q(x)$ be the PDF under the $\mathcal{H}_1$ assumption, then the K-L distance is

$$\begin{aligned} D_{\mathrm{KL}}(P||Q) &= -\frac{1}{2} + \frac{\sigma_n^2}{2\left(\sigma_\eta^2+\sigma_n^2\right)} + \log\left(\frac{\sigma_\eta^2+\sigma_n^2}{\sigma_n^2}\right) \\ &= \frac{-\xi}{2(1+\xi)} + \log(1+\xi) \simeq \frac{\xi}{2}, \quad \text{when } \xi \to 0. \end{aligned} \tag{31}$$

From the point of view of K-L distance, the power of the modulated signal is much lower than the noise power, the more favorable the concealment is.

4.2 BER under AWGN Channels

From the definition of SNR and the variance of the carrier being 1, the variance of the noise is obtained as $\sigma_n^2 = \xi^{-1}$. The interference component z_{i} of the correlator output obeys the $\mathcal{N}\left(0, \sigma_{z_{\mathrm{i}}}^2\right)$ distribution, where $\sigma_{z_{\mathrm{i}}}^2 = (2\xi^{-1} + \xi^{-2})\nu^{-1}$. The higher the SNR, the smaller the variance of the interference component and the smaller the effect on the BER.

Equation (15) gives the mean and variance of the correlator output, combined with the condition that the variance of the carrier $\sigma_\eta^2 = 1$, yields $\mu_z = (-1)^b\rho$, where the covert bit $b \in \{0, 1\}$. Thus the probability density function is further simplified to

$$f_z(z|b) = \frac{1}{\sqrt{2\pi}\sigma_z}\mathrm{e}^{-\frac{\left(z-(-1)^b\rho\right)^2}{2\sigma_z^2}} \tag{32}$$

where $\sigma_z^2 = \nu^{-1}\left(1+\rho^2+2\xi^{-1}+\xi^{-2}\right)$. Demodulation is done by a simple hard decision, i.e., the covert bit is estimated as

$$\hat{b} = \begin{cases} 0, & z \geq 0 \\ 1, & z < 0 \end{cases}. \tag{33}$$

Assuming that the "0" and "1" covert bits sent are of equal probability, namely $\Pr(b=0) = \Pr(b=1) = \frac{1}{2}$, and combining (32) and (33), the bit error rate is obtained as

$$\begin{aligned} P_{\mathrm{e}} &= \frac{1}{2}\int_0^{\infty} f_z(z|b=1)\mathrm{d}z + \frac{1}{2}\int_{-\infty}^{0} f_z(z|b=0)\mathrm{d}z \\ &= \int_0^{\infty} f_z(z|b=1)\mathrm{d}z = \frac{1}{2}\mathrm{Erfc}\left(\frac{\rho}{\sqrt{2\sigma_z^2}}\right) \\ &= \frac{1}{2}\mathrm{Erfc}\left(\sqrt{\frac{\rho^2\nu/2}{1+\rho^2+2\xi^{-1}+\xi^{-2}}}\right). \end{aligned} \tag{34}$$

4.3 BER under Quasi-static Fading Channels

In Sec. 3.3, the PDF of the correlator output z under quasi-static fading channels is obtained (cf. (22)). With the carrier variance set to 1, this is further simplified as

$$f_z(z|h,b) = \frac{1}{\sqrt{2\pi}\sigma_z}\mathrm{e}^{-\frac{\left(z-(-1)^b h^2\rho\right)^2}{2\sigma_z^2}} \tag{35}$$

where the variance of z is also simplified as (cf. (21))

$$\sigma_z^2 = \nu^{-1}\left(h^4\left(1+\rho^2\right)+2h^2\sigma_n^2+\sigma_n^4\right). \tag{36}$$

Considering that $\Pr(b=1) = \Pr(b=0) = 1/2$, the demodulation still uses hard decision (as shown in (33)), then the BER P_{e} is

$$\begin{aligned} P_{\mathrm{e}} &= \mathbb{E}_h\left[\int_0^{\infty} f_z\left(z|h,b=1\right)\mathrm{d}z\right] \\ &= \mathbb{E}_h\left[\int_0^{\infty}\frac{1}{\sqrt{2\pi}\sigma_z}\mathrm{e}^{-\frac{(z+\mu_z)^2}{2\sigma_z^2}}\mathrm{d}z\right] = \mathbb{E}_h\left[\frac{1}{2}\mathrm{Erfc}\left(\frac{\rho h^2}{\sqrt{2\sigma_z^2}}\right)\right] \\ &= \frac{1}{2}\int_0^{\infty}\mathrm{Erfc}\left(\frac{\rho h^2}{\sqrt{2\sigma_z^2}}\right) f_h(h)\mathrm{d}h \\ &= \frac{1}{2}\int_0^{\infty}\mathrm{Erfc}\left(\sqrt{\frac{\rho^2 h^4\nu/2}{h^4\left(1+\rho^2\right)+2h^2\sigma_n^2+\sigma_n^4}}\right) f_h(h)\mathrm{d}h. \end{aligned} \tag{37}$$

In general, there does not exist a closed-form analytic expression for (37).

The channel model is assumed to be a frequency-flat Rayleigh fading channel without Doppler shift, and the channel fading coefficient h obeys a Rayleigh distribution with parameter β, i.e.,

$$f_h(h) = \frac{h}{\beta^2}\exp\left(-\frac{h^2}{2\beta^2}\right). \tag{38}$$

As an example, the transmitter selects a Gaussian stochastic process as the carrier, and in the following, we analyze the BER performance of the proposed covert system under quasi-static Rayleigh flat fading channels.

Define the SNR as the ratio of the power of the receiver signal to the power of the noise, and apply the law of total expectation under the condition of carrier unit variance to obtain the SNR

$$\begin{aligned} \xi &= \frac{\mathbb{E}\left[h^2\lambda_k^2\right]}{\sigma_n^2} = \frac{\mathbb{E}_h\left[\mathbb{E}_\lambda\left[h^2\lambda_k^2|\lambda_k\right]\right]}{\sigma_n^2} = \frac{\sigma_\eta^2\mathbb{E}_h[h^2]}{\sigma_n^2} \\ &= \frac{2\beta^2\sigma_\eta^2}{\sigma_n^2} = \frac{2\beta^2}{\sigma_n^2} \quad \Rightarrow \quad \sigma_n^2 = 2\beta^2\xi^{-1}. \end{aligned} \tag{39}$$

Substituting (38) and (39) into (37), we get the BER under Rayleigh fading channel as

$$P_{\mathrm{e}} = \frac{1}{2}\int_0^{\infty}\mathrm{Erfc}\left(\sqrt{\frac{\rho^2 h^4\nu/2}{h^4\left(1+\rho^2\right)+4h^2\beta^2\xi^{-1}+4\beta^4\xi^{-2}}}\right)\frac{h}{\beta^2}\exp\left(-\frac{h^2}{2\beta^2}\right)\mathrm{d}h. \tag{40}$$

For comparison with the BER under AWGN channels, the fading average power is set to 1 so that the assumed fading channel obeys a Rayleigh distribution with parameter $\beta = \sqrt{1/2}$. The BER under the fading channel is correspondingly rewritten as

$$P_{\mathrm{e}} = \int_0^{\infty}\mathrm{Erfc}\left(\sqrt{\frac{\rho^2 h^4\nu/2}{h^4\left(1+\rho^2\right)+2h^2\xi^{-1}+\xi^{-2}}}\right)h\mathrm{e}^{-h^2}\mathrm{d}h. \tag{41}$$

5. Correlation Detection and Pseudo-random Sequences

In this section, we specifically address the problem of eavesdroppers sensing the presence of covert signals through correlation detection. To solve this problem, a pseudo-random sequence generator is added to the transmitter of Fig. 1. Finally, the receiver synchronizes the pseudo-random sequence utilizing correlation detection.

5.1 Correlation Detection

The signals that have been modulated with covert bits have a very pronounced periodicity, which exposes the existence of covert bit period as well as covert communication. To better illustrate this issue, the modulation process is redrawn as shown in Fig. 4. In the figure, we assume that the stochastic process $\eta(t)$ as a carrier has the statistical properties of having a mean of 0, a variance of σ_η^2, and an autocorrelation function of $\mathbb{E}[\eta(t)\eta(s)] = R_\eta(t,s) = \sigma_\eta^2\delta(t-s)$. Here $\lambda(t) = \eta(t)$ serves as the reference carrier and contains no covert bit. Assume further that $\eta(t+kT_{\mathrm{b}}), \lambda(t+kT_{\mathrm{b}})$ are the carrier and the modulated signal of the kth covert bit, respectively.

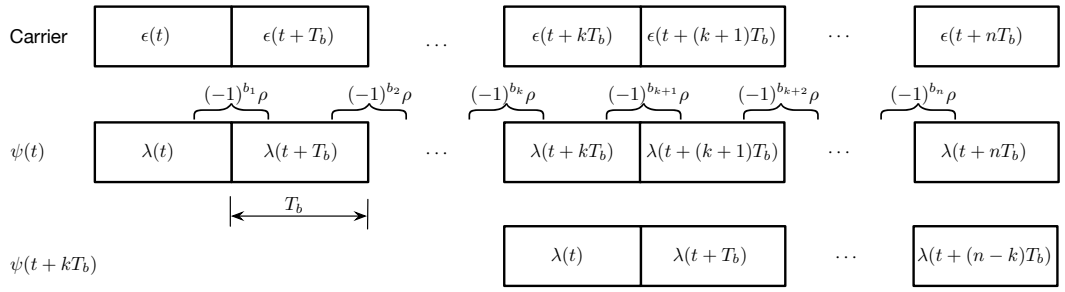


Fig. 4. Illustrative diagram of carriers and covert signals.

From the Fig. 4, it can be seen that the modulated signal $\psi(t)$ for the first n covert bits can be written as

$$\psi(t) = \sum_{i=0}^{n} \lambda(t + iT_{\mathrm{b}}) = \sum_{i=0}^{n} \lambda_i. \tag{42}$$

The autocorrelation function (ACF) of the modulated signal $\psi(t)$ is defined as

$$R_\psi(\tau) = \mathbb{E}[\psi(t)\psi(t+\tau)]. \tag{43}$$

When τ is not an integer multiple of the bit period, $\tau \neq kT_{\mathrm{b}}$, it is clear that there is $R_\psi(\tau) = 0$ due to the carrier stochastic process's ACF $R_\epsilon(\tau) = \mathbb{E}[\epsilon(t)\epsilon(t+\tau)] = \sigma_\eta^2\delta(\tau)$. We derive in detail the autocorrelation coefficient of the modulated signal $\psi(t)$ when $\tau = kT_{\mathrm{b}}$ as follows.

First, to simplify the description of the problem, we assume that the covert bits sent are all zeros. Hence, Equation (4) is reduced to

$$\begin{cases} \lambda_0 = \epsilon_0 \\ \lambda_1 = \rho\epsilon_0 + \sqrt{1-\rho^2}\epsilon_1 \\ \quad\vdots \\ \lambda_k = \rho^k\epsilon_0 + \sum_{i=1}^{k} \rho^{k-i}\sqrt{1-\rho^2}\epsilon_i \\ \quad\vdots \end{cases}. \tag{44}$$

Second, based on (7) , we obtain the variance of the modulated signal $\psi(t)$ as

$$\sigma_\psi^2 = R_\psi(0) = \mathbb{E}\left[\sum_{i=0}^{n} \lambda_i^2\right] = (n+1)\sigma_\eta^2. \tag{45}$$

Third, referring to Fig. 4, we obtain the ACF of the modulated signal $\psi(t)$ when $\tau = kT_{\mathrm{b}}$ as

$$\begin{aligned} R_\psi(kT_{\mathrm{b}}) &= \mathbb{E}\left[\psi(t)\psi(t+kT_{\mathrm{b}})\right] = \sum_{i=0}^{n-k} \mathbb{E}\left[\lambda_i\lambda_{k+i}\right] \\ &= \sum_{i=0}^{n-k} \mathbb{E}\left[\lambda_i \underbrace{\left(\rho^k\lambda_i + \sqrt{1-\rho^2}\sum_{l=1}^{k}\rho^{k-l}\epsilon_{i+l}\right)}_{\lambda_{k+i}}\right] \\ &= \sigma_\eta^2 \sum_{i=0}^{n-k} \rho^k = \rho^k(n-k+1)\sigma_\eta^2 \end{aligned} \tag{46}$$

where the mutual independent of λ_i and ϵ_{i+l} is used, i.e., $\mathbb{E}[\lambda_i\epsilon_{i+l}] = 0$.

Finally, we obtain the normalized autocorrelation coefficient of the modulated signal $\psi(t)$ as

$$\begin{aligned} \rho_\psi(\tau) = \frac{R_\psi(\tau)}{\sigma_\psi^2} &= \begin{cases} 0 & \text{for} \quad \tau \neq kT_{\mathrm{b}} \\ \left(1 - \frac{k}{n+1}\right)\rho^k & \text{for} \quad \tau = kT_{\mathrm{b}} \end{cases} \\ &= \left(1 - \frac{k}{n+1}\right)\rho^k\delta(\tau - kT_{\mathrm{b}}) \\ &= \left(1 - \frac{|k|}{n+1}\right)\rho^{|k|}\delta(\tau - kT_{\mathrm{b}}) \quad \text{for } |k| \leq n \end{aligned} \tag{47}$$

where the last equation is established by the symmetry of the correlation coefficients.

From (47), it can be seen that there is a significant autocorrelation of the modulated signals $\psi(t)$. Therefore, if an eavesdropper intercepts the transmitter's signal, and then uses correlation analysis to reveal the existence of covert communications. To visualize this problem more, we demonstrate it with MATLAB simulation. The carrier sequence after modulation by a covert bit stream (all covert bits are 0) is shown in Fig. 5 together with the normalized autocorrelation sequences for the modulated signals. The autocorrelation function "xcorr" of the MATLAB software is used here to compute the normalized correlation sequences of the modulated signals.

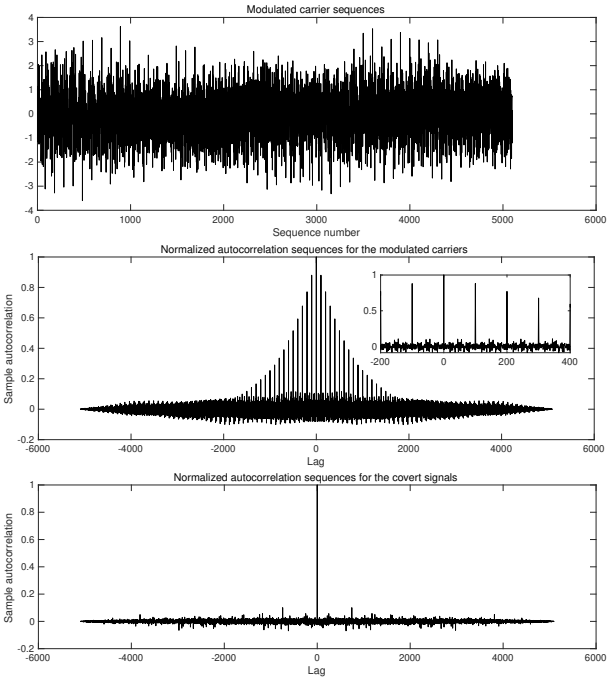


Fig. 5. Modulated signal sequences and its normalized autocorrelation sequences, where all covert bits are 0, the carrier uses Gaussian noise with a mean of 0 and variance of 1, the correlation coefficient $\rho = 0.9$, the number of samples in a covert bit period $\nu = 100$, the pseudo-random sequence period $m = 31$, and the number of covert bits $n = 50$.

5.2 Pseudo-random Sequences

To avoid this problem and to increase the difficulty for eavesdroppers to sense the existence of covert communications, a pseudo-random generator is introduced in this work. The carrier sequences, modulated by a covert bitstream, are multiplied with the pseudo-random sequences and then transmitted to the channel as covert signals. The "comm.PNSequence" function of the MATLAB software is used to generate the pseudo-noise (PN) sequence. The generating polynomial for the PN sequence is x^5+x^2+1. As shown in Fig. 5, the autocorrelation of the covert signal has disappeared, thus increasing the difficulty for the eavesdropper to perceive the presence of the covert signal. After the multiplication of a pseudo-random sequence, the covert signal's autocorrelation coefficient is derived as follows.

Let m be the pseudo-random sequence period, then the normalized autocorrelation coefficient of the PN sequence is approximately $\rho_{\mathrm{PN}}(\tau) = \delta(\tau - m)$. Let $\mathrm{LCM}(a, b)$ be the least common multiple of a and b. In particular, when a and b are prime, $\mathrm{LCM}(a, b) = ab$. In this work, the number of samples in a bit period is v and the period of the pseudo-random sequence is m, then it is easy to choose v and m such that $\mathrm{LCM}(v, m) = vm$. Since the pseudo-random sequences and the modulated sequences are mutually independent stochastic processes, the normalized autocorrelation coefficient of the covert signal sequences can be obtained directly from (47), which is rewritten as

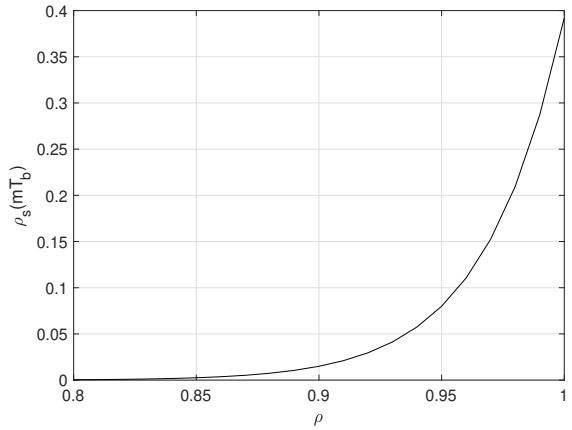


Fig. 6. Relationship between the normalized correlation coefficient $\rho_\psi(mT_\mathrm{b})$ of the first period of the covert signal and the correlation coefficient ρ, where $\nu = 100$, $m = 31$, $n = 50$.

$$\begin{aligned}\rho_\psi(\tau) &= \left(1 - \frac{|\tau|/\nu}{n+1}\right)\rho^{|\tau|/\nu}\delta(\tau - k\nu)\delta(\tau - m)\\ &= \left(1 - \frac{|\tau|/\nu}{n+1}\right)\rho^{|\tau|/\nu}\delta\left(\tau - k\mathrm{LCM}(\nu, m)\right)\\ &= \left(1 - \frac{|k|m}{n+1}\right)\rho^{|k|m}\delta(\tau - km\nu)\end{aligned} \tag{48}$$

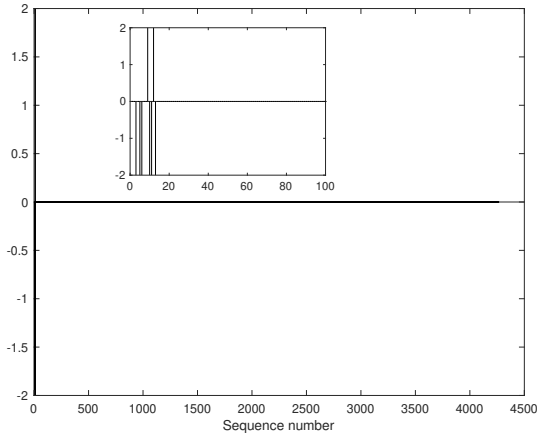
when $|k|m \le n$. Following the parameters set in Fig. 5, we get $\mathrm{LCM}(v, m) = 3100$, i.e., the first periodicity of the covert signal does not appear until the 31st-bit period. However, the correlation coefficient at this moment is $(1-m/(n+1))\rho^m = 0.015$, which can be considered completely uncorrelated, especially in the presence of channel noise, since the correlation coefficient is even smaller. As a result, the covert signal after the pseudo-random sequence processing is not relevant anymore. Hence, it is difficult for an eavesdropper to use the correlation to sense the presence of covert communication.

Figure 6 illustrates the relationship between the normalized correlation coefficient $\rho_\psi(mT_\mathrm{b}) = \left(1 - \frac{m}{n+1}\right)\rho^m$ of the first period of the covert signal and the correlation coefficient ρ of the adjacent two-bit periods. We choose suitable ν and m such that on the one hand the correlation period of the covert signal becomes very long, and on the other hand the correlation becomes very small, thus very favorable to the covertness of the transmitted signal. At the same time, we choose the correlation coefficient ρ as large as possible, since this will reduce the BER of the communication system.

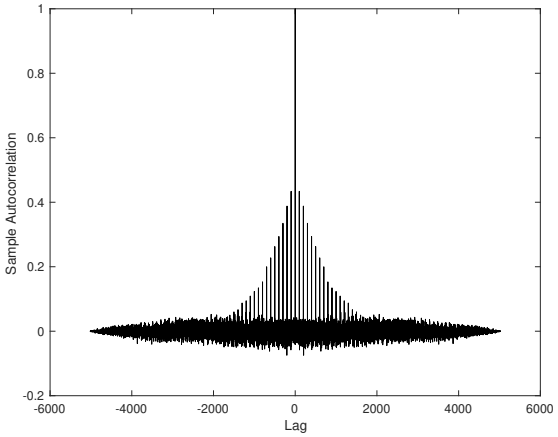
5.3 Synchronization

The receiver must make the local pseudo-random sequence synchronized with the transmitter's pseudo-random sequence before performing the correlation demodulation. In the modulation-demodulation scheme proposed in this work, due to the short period of the pseudo-random sequence (e.g., $m = 31$), the brute force exhaustive method can be used for pseudorandom sequence synchronization.

It is assumed that $n = 50$ zeros are used by both legitimate communicating parties for the synchronization sequence of the pseudo-random sequence. The simulation parameters are the same as in Fig. 5, resulting in a total of $(n+1)\nu = 5100$ samples of the synchronized signal. Assuming that the receiver loses the first 840 samples, the receiver uses brute-force exhaustion to recover the synchronization of the pseudo-random sequence. The SNR of the AWGN channel is 0 dB. The receiver first generates a pseudo-random sequence of the same length as the received signal samples, then multiplies the pseudo-random sequence with the received signal samples, and finally performs a normalized autocorrelation for this sequence. The receiver determines whether it has been synchronized on the fact that more than 5 autocorrelation coefficients are greater than a certain threshold (e.g. 0.3). If it is judged to be unsynchronised, the pseudo-random sequence is circularly shifted by one chip position. The synchronized pseudo-random sequence is found after at most $m = 31$ attempts.



(a) Difference between the pseudo-random sequence recovered at the receiver and the pseudo-random sequence at the transmitter



(b) Normalized autocorrelation sequence of received signals after synchronization of pseudo-random sequences

Fig. 7. Resynchronization of pseudo-random sequences, where the parameters of the simulation are the same as in Fig. 5, with an offset of 840 samples, i.e., $8.4T_\mathrm{b}$ and SNR $\xi = 0$ dB.

As can be seen from Fig. 7, the recovered pseudo-random sequence is out of sync with the transmitter's pseudo-random sequence in the first dozen chips, but then it is completely synchronized. This is caused by the length of the received signal not being an integer multiple of the length of the pseudo-random sequence. From the setting of the simulation parameters, there exists a synchronous code-chip error of $\mathrm{Mod}((n+1)\nu - 840, m) = \mathrm{Mod}(5100 - 840, 31) = 13$, which is consistent with the results of the simulation.

6. Simulation and Analysis

The BER of the proposed differential stochastic process keying system is simulated using MATLAB software and compared with the theoretically derived results. The simulation system constructed is shown in Fig. 1, which mainly consists of modulation, channel, demodulation, and BER statistics modules. The simulation parameters are shown in Tab. 2.

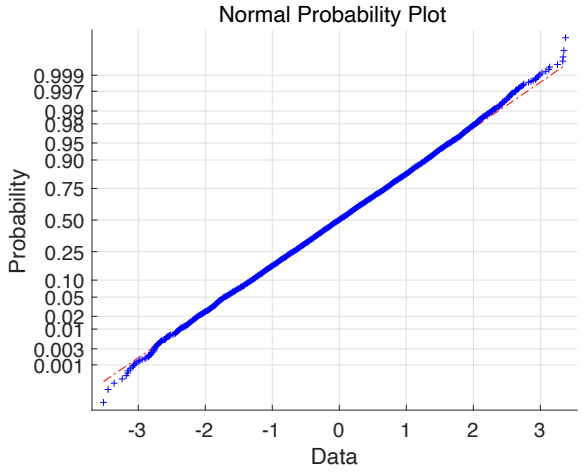
A stochastic process generator generates the carrier, and four random processes, namely, uniform, Gaussian, exponential, and Rayleigh distributions, are chosen in the simulation. A Bernoulli binary random number generator generates the covert source, and equal probability '0' and '1' bit streams are mapped to $\{-1, +1\}$, which are then used to control the polarity of the correlation coefficients of the two adjacent stochastic carrier sequences. The channel consists of Rayleigh fading multiplied by the modulating signal and summed Gaussian white noise, with the fading coefficients remaining constant over two covert bit periods. If the fading of the channel is not considered, simply set the fading coefficient to 1. In the receiver, differential demodulation is used to obtain an estimate of the transmitted bits after hard decision, and then the BER of the system is obtained by comparison and statistics. During demodulation in the receiver, it is assumed that synchronization has been obtained.

First, we verify that the modulation signal λ_k of the kth covert bit (i.e. Eq. (6) in Sec. 3.1) obeys a normal distribution from three aspects. Although a uniform-distributed stochastic process is used for the carrier, the modulated signal after multiple covert bits shows a normal distribution, which is the power of the central limit theorem, as shown in Fig. 8.

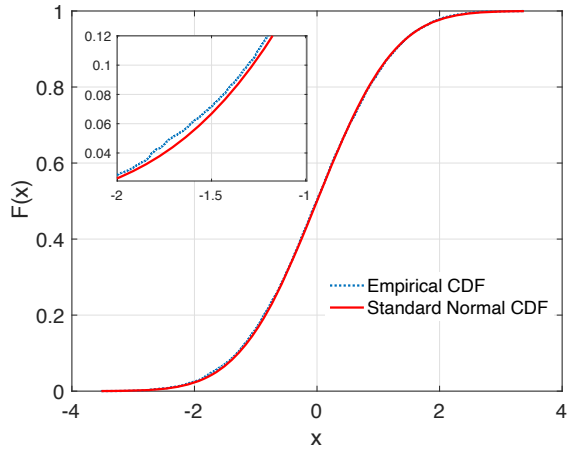
The purpose of introducing the "normplot" function of the MATLAB software in the study is to evaluate how close the random variable is to the normal distribution. The plot will be linear if the sample data are normal, otherwise, other distributions will introduce curvature.

Carrier	Uniform/Normal/Exponential/Rayleigh
n	Number of covert bits
T_b	Covert bit period
ν	Number of samples in T_b
ξ	SNR
ρ	Correlation coefficient
Fading PDF	$f_h(h) = 2he^{-h^2}, x \geq 0$

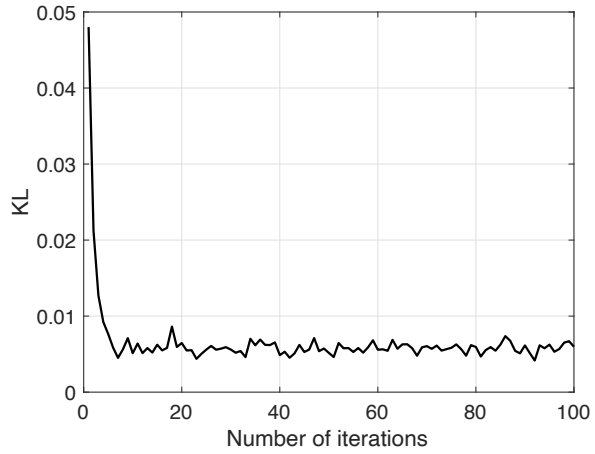
Tab. 2. Simulation parameters.



(a) Normal probability plot



(b) Kolmogorov-Smirnov (K-S) test



(c) Kullback-Leibler divergence between the standard normal PDF and approximate PDF of the modulated signal

Fig. 8. Normal probability plot, K-S test and K-L divergence of the modulated signals for the n-th covert bit, when a uniform-distributed stochastic process is used as the carrier, where the correlation coefficient $\rho = 0.9$, the number of samples in a covert bit period $\nu = 10^4$, and the number of covert bits $n = 100$.

In Fig. 8(a), the plot has the sample data displayed with the plot symbol '+', and a line joining the first and third quartiles of the sample data is superimposed on the plot. The modulated signal of the 100th covert bit fits the normal distribution very well.

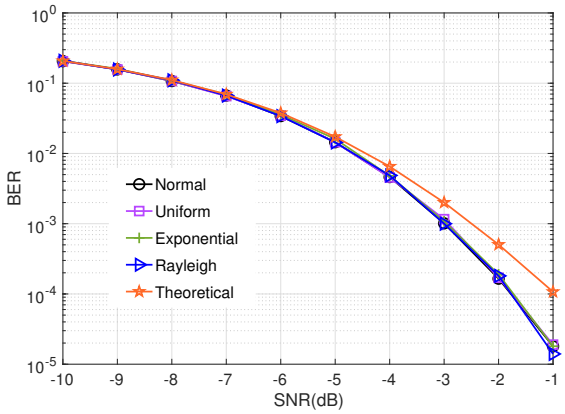
The one-sample Kolmogorov-Smirnov test [30] is used to test the goodness of fit of a given set of data to a theoretical distribution. The one-sample Kolmogorov-Smirnov test was performed using MATLAB software's "kstest" function. Test decisions were confirmed by visually comparing the empirical cumulative distribution function (CDF) with the standard normal CDF. As shown in Fig. 8(b), the two curves are very close together.

Kullback-Leibler divergence (K-L) is used to measure statistics that quantify the proximity of two probability distributions in the same event space. Here, let $p(x)$ be the empirical PDF of the modulated signal and $q(x)$ be the PDF of the standard normal distribution in (30). As can be seen from Fig. 8(c), the modulated signal after 5 or 6 covert bits, the K-L distance decreases dramatically and tends to 0, which indicates that the modulated signal obeys a normal distribution.

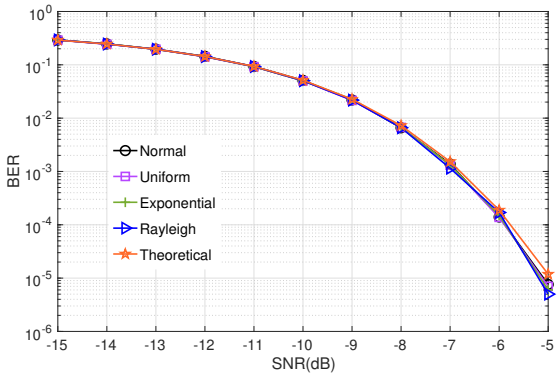
Second, we examine the BER performance of the system under AWGN channels. Due to the requirement of covertness, the power of the transmitted covert signal must be less than the power of the channel noise, that is, the SNR is less than 0 dB. We examine the BER performance when the number of samples in a bit period is $\nu = 100$, 400 and 1000, respectively. Stochastic uniform, normal, exponential, and Rayleigh distribution processes are used as carriers. The covert bitstream is randomly generated with equal probability. As can be seen from Fig. 9, no matter which carrier uses a stochastic process, their BERs are very close to each other, which is consistent with our theoretical analysis.

Interestingly, when the number of samples in a covert bit period $\nu = 100$, the simulation yields a better performance than that derived by theory within the periods of the SNR $[-5, -1]$ dB, which may be because ν is not sufficiently large, resulting in the output of the correlator not completely following the normal distribution. On the one hand, when the SNR is low, e.g. -15 dB, increasing ν does little effect on reducing BER and results in a reduction in transmission rate. On the other hand, when the SNR is large, then increasing ν has a very significant effect on reducing BER.

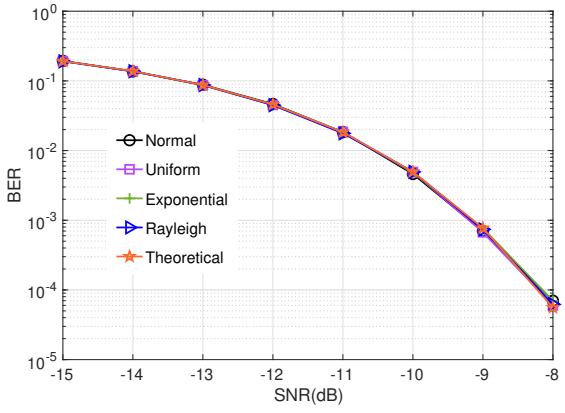
$$\begin{aligned} P_{\mathrm{e}} &= \int_0^{\infty} \mathrm{Erfc}\left[0.9h^2\sqrt{\frac{\nu/2}{1.81h^4+2h^2+1}}\right] h\mathrm{e}^{-h^2}\mathrm{d}h \\ &= \int_0^{1} [\cdot]\,\mathrm{d}h + \underbrace{\int_1^{\infty} [\cdot]\,\mathrm{d}h}_{1.456510^{-18}} \\ &\approx \int_0^{1} \mathrm{Erfc}\left[0.9h^2\sqrt{\frac{\nu/2}{1.81h^4+2h^2+1}}\right] h\mathrm{e}^{-h^2}\mathrm{d}h. \end{aligned} \tag{49}$$



(a) $\nu = 100$



(b) $\nu = 400$



(c) $\nu = 1000$

Fig. 9. Theoretical versus simulated BER with $\rho = 0.9$ under AWGN channels.

Third, we examine the BER performance of the system under Rayleigh fading channels, shown in Fig. 10. The theoretical BER is numerically calculated from (41). The BER curves of these four distributions are very close, and the theory is consistent with the simulation. The stochastic process with normal carrier distribution, sampling number $\nu = 400$, SNR $\xi = 0$ dB is an example to explain why the BER is relatively high in the fading channel. As can be seen from (49), the larger the fading amplitude h, the smaller the value of the function Erfc(h). Conversely, the smaller the fading amplitude h, the greater the value of the function Erfc(h).

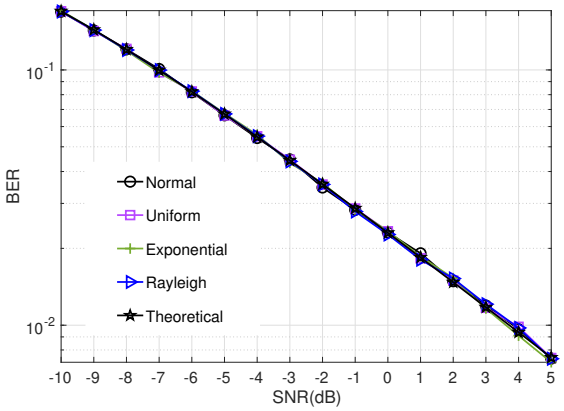


Fig. 10. Theoretical versus simulated BER with $\rho = 0.9$, $\nu = 400$ under Rayleigh fading channels.

Therefore, the BER is mainly caused by the fading of $h < 1$. When $h < 0.2$, the Erfc[] value is near 1 and $he^{-h^2} \approx h$, so P_e is at least greater than $\int_0^{0.2} h dh = 0.02$.

7. Conclusion

In this work, a modulation and demodulation structure, which is called differential stochastic process keying covert communication, is proposed. The proposed scheme has a good concealment nature. The stochastic process is used as the carrier, the transmitted bits are "hidden" in the noise-like carrier, and the statistical characteristics of the waveforms of the transmitted '0' and '1' bits are the same. The statistical characteristics of the transmitted '0' and '1' bit waveforms are identical. The proposed scheme is simple in structure and low in complexity. No carrier recovery is required at the receiver and the transmitted covert bit can be estimated just by a simple correlator and hard decision. The proposed scheme has a low BER performance. The theoretical derivation and simulation show that the BER is as low as 10^{-3} for an SNR of about -3 dB and a bit-period sampling number of $\nu = 100$ under the AWGN channel. The proposed system works at the physical layer with good security, flexibility, and BER performance. It is well suited for IoT devices with limited resources and low transmission rate requirements but high concealability requirements.

Acknowledgments

This work was supported in part by "Pioneer" and "Leading Goose" R&D Program of Zhejiang (Grant No. 2023C01030), in part by the National Natural Science Foundation of China (Grant No. 62071212 and 62371218), and in part by the open project of Guangdong Provincial Key Laboratory of Advanced Wireless Communications (Southern University of Science and Technology, Shenzhen 518055, China).

References

[1] CHEN, X., AN, J., XIONG, Z., et al. Covert communications: a comprehensive survey. *IEEE Communications Surveys and Tutorials*, 2023, vol. 25, no. 2, p. 1171–1198. DOI: 10.1109/COMST.2023.326391

[2] SHEN, Y., ZHANG, Y., JIANG, X. *Secrecy, Covertness, and Authentication in Wireless Communications: Physical Layer Security Approach*. Cham (Switzerland): Springer, 2023. ISBN: 9783031384646

[3] YANG, N., WANG, L., GERACI, G., et al. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine*, 2015, vol. 53, no. 4, p. 20–27. DOI: 10.1109/MCOM.2015.7081071

[4] PENG, J., TANG, S. Covert communication over VoIP streaming media with dynamic key distribution and authentication. *IEEE Transactions on Industrial Electronics*, 2021, vol. 68, no. 4, p. 3619–3628. DOI: 10.1109/TIE.2020.2979567

[5] YENER, A., ULUKUS, S. Wireless physical-layer security: Lessons learned from information theory. *Proceedings of the IEEE*, 2015, vol. 103, no. 10, p. 1814–1825. DOI: 10.1109/JPROC.2015.2459592

[6] LIU, Z. H., LIU, J.J., ZENG, Y., et al. Covert wireless communications in IoT systems: Hiding information in interference. *IEEE Wireless Communications*, 2018, vol. 25, no. 6, p. 46–52. DOI: 10.1109/MWC.2017.1800070

[7] BASH, B. A., GOECKEL, D., TOWSLEY, D. Limits of reliable communication with low probability of detection on AWGN channels. *IEEE Journal on Selected Areas in Communications*, 2013, vol. 31, no. 9, p. 1921–1930. DOI: 10.1109/JSAC.2013.130923

[8] AZERANG, S.F., SAMSAMI KHODADAD, F., FOROUZESH, M. Covert communication based on energy harvesting and cooperative jamming. *Wireless Networks*, 2022, vol. 28, p. 3729–3738. DOI: 10.1007/s11276-022-03082-x

[9] TA, H. Q, PHAM, Q. V., KHUONG, H. V., et al. Covert communication with noise and channel uncertainties. *Wireless Networks*, 2022, vol. 28, p. 161–172. DOI: 10.1007/s11276-021-02828-3

[10] HUANG, S. H., LIU W. W., LIU, G. J., et al. A correlation-based approach to detecting wireless physical covert channels. *Computer Communications*, 2021, vol. 76, p. 31–39. DOI: 10.1016/j.comcom.2021.05.017

[11] CHEN, X., ZHENG, T. X., DONG, L. M., et al. Enhancing MIMO covert communications via intelligent reflecting surface. *IEEE Wireless Communications Letters*, 2022, vol. 11, no. 1, p. 33–37. DOI: 10.1109/LWC.2021.3119687

[12] HU, L. T., BI, S. J., LIU, Q. J., et al. Intelligent reflecting surface aided covert wireless communication exploiting deep reinforcement learning. *Wireless Networks*, 2023, vol. 29, p. 877–899. DOI: 10.1007/s11276-022-03037-2

[13] LI, M., TAO, X. F., LI, N., et al. Energy-efficient covert communication with the aid of aerial reconfigurable intelligent surface. *IEEE Communications Letters*, 2022, vol. 26, no. 9, p. 2101–2105. DOI: 10.1109/LCOMM.2022.3183637

[14] LI, Q., XU, D. Y., ZHANG, K. Y., et al. Covert communications in STAR-RIS assisted NOMA IoT networks over Nakagami-m fading channels. *IEEE Internet of Things Journal*, 2024, vol. 11, no. 12, p. 22456–22470. DOI: 10.1109/JIOT.2024.3381596

[15] GAO, C., YANG, B., JIANG, X. H., et al. Covert communication in relay-assisted IoT systems. *IEEE Internet of Things Journal*, 2021, vol. 8, no. 8, p. 6313–6323. DOI: 10.1109/JIOT.2021.3051694

[16] ZHAO, Q. X., GAO, C., ZHENG, D., et al. Covert communication in a multirelay-assisted wireless network with an active warden. *IEEE Internet of Things Journal*, 2024, vol. 11, no. 9, p. 16450–16460. DOI: 10.1109/JIOT.2024.3353833

[17] WAN, Z. H., HUANG, Y., LEI, J., et al. Energy-efficient covert communication with adaptive assist nodes group. *IET Communications*, 2023, vol. 17, no. 7, p. 797–806. DOI: 10.1049/cmu2.12583

[18] CHEN, W., Y., DING, H. Y., HU, L., et al. Covert communication based on noise uncertainty against multi-antenna detection: Analyses of limit covert and reliable rate. *IEEE Wireless Communications Letters*, 2024, vol. 13, no. 1, p. 148–152. DOI: 10.1109/LWC.2023.3323764

[19] HU, J. S., YAN, S. H., ZHOU, X. B., et al. Covert communications without channel state information at receiver in IoT systems. *IEEE Internet of Things Journal*, 2020, vol. 7, no. 11, p. 11103–11114. DOI: 10.1109/JIOT.2020.2994441

[20] SOLTANI, R., GOECKEL, D., TOWSLEY, D., et al. Covert wireless communication with artificial noise generation. *IEEE Transactions on Wireless Communications*, 2018, vol. 17, no. 11, p. 7252–7267. DOI: 10.1109/TWC.2018.2865946

[21] LI, L. T., CHEN, Z. L., CHEN, R. Q., et al. Covert wireless communication with random frequency diverse array. *IEEE Transactions on Vehicular Technology*, 2024, vol. 73, no. 1, p. 1473–1478. DOI: 10.1109/TVT.2023.3310986

[22] CEK, M. E., SAVACI, F. A. Stable non-Gaussian noise parameter modulation in digital communication. *Electronics Letters*, 2009, vol. 45, no. 24, p. 1256–1257. DOI: 10.1049/el.2009.2280

[23] CEK, M. E. Covert communication using skewed α-stable distributions. *Electronics Letters*, 2015, vol. 51, no. 1, p. 116–118. DOI: 10.1049/el.2014.3323

[24] AHMED, A., SAVACI, F. A. Blind recognition of alpha-stable random carrier signals by an eavesdropper in random communication systems. *IET Communications*, 2019, vol. 13, no. 16, p. 2420–2427. DOI: 10.1049/iet-com.2018.5884

[25] SAVACI, F. A., AHMED, A. Inverse system approach to design alpha-stable noise driven random communication system. *IET Communications*, 2020, vol. 14, no. 6, p. 910–913. DOI: 10.1049/iet-com.2018.5702

[26] XU, Z. J., GONG, Y., WANG, K., et al. Covert digital communication systems based on joint normal distribution. *IET Communications*, 2017, vol. 11, no. 8, p. 1282–1290. DOI: 10.1049/iet-com.2016.1333

[27] XU, Z. J., LU, W. D., GONG, Y., et al. A covert communication system using non-zero mean normal distributions. *Radioengineering*, 2020, vol. 29, no. 3, p. 580–588. DOI: 10.13164/re.2020.0580

[28] BASAR, E. Noise modulation. *IEEE Wireless Communications Letters*, 2024, vol. 13, no. 3, p. 844–848. DOI: 10.1109/LWC.2023.3346471

[29] SHLENS, J. Notes on Kullback-Leibler divergence and likelihood theory. *arXiv*, 2014, p. 1–4. DOI: 10.48550/arXiv.1404.2000

[30] LOPES, R.H.C. *Kolmogorov-Smirnov Test.* In: *Lovric, M. (eds) International Encyclopedia of Statistical Science*. Berlin Heidelberg (Germany): Springer, 2011. DOI: 10.1007/978-3-642-04898-2_326

About the Authors ...

Zhijiang XU (corresponding author) was born in 1973. He received his Ph.D. in Information and Communication Engineering in 2005 from Zhejiang University, China. He was appointed associate professor in the College of Information Engineering at Zhejiang University of Technology, China, from 2007 to 2019. Since 2019, he has joined the Zhejiang Institute of Mechanical & Electrical Engineering in the School of Automation and was promoted to Full Professor in 2020. His research interests include digital communications over fading channels, channel modeling, coding, digital synchronization, etc.

Yi GONG was born in 1973. He received his Ph.D. in Electrical Engineering from the Hong Kong University of Science and Technology, Hong Kong 2002. He then joined the Hong Kong Applied Science and Technology Research Institute, Hong Kong, as a Member of the Professional Staff. He is now a Professor at the Southern University of Science and Technology, Shenzhen, China. Before his current appointment, he was employed at Nanyang Technological University, Singapore, where he still has active collaborations. Since 2006, he has served on the editorial board of the IEEE Transactions on Wireless Communications and the IEEE Transactions on Vehicular Technology. His research interests include cognitive radio, full-duplex communications, wireless energy harvesting, and physical layer security for wireless systems.